Audit and Accountability

**AU-1: Audit and Accountability Policy and Procedures**

NIST SP 800-53 Objective: The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

b. Reviews and updates the current:

1. Audit and accountability policy [Assignment: organization-defined frequency]; and

2. Audit and accountability procedures [Assignment: organization-defined frequency].

Control Translation: This control is to ensure that the organization has created audit and accountability policies and procedures that are organizational specific, available to all required personnel, and updated to ensure accuracy and contain specific information regarding the organization.

Notes: The organizational risk management strategy is a key factor in the development of the access control policy and procedures. Related control: PM-9. This control can be applied at the General level.

How to test and evaluate: Examine SSP and Audit and Accountability Policy and Procedures. Verify that the policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance of organization/agency. Ensure audit and accountability policy and procedures are in place, sent to the organization defined personnel, and are updated in accordance with the organization defined time frame.

Technology specific: General

**AU-2: Audit Events**

NIST SP 800-53 Objective: The organization:

a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

Control Translation: This control is to ensure that the organization has clearly defined the events that are to be audited by all components across the organization.

How to test and evaluate: Examine SSP and Audit and Accountability Policy and Procedures. Determine if the organizational policies clearly state the events to be audited by all components across the organization. Interview the key point of contact to ensure auditing activities and incidents are recorded in the ticket system to ensure availability to all necessary personnel. Obtain 5 tickets to show that audit incidents and suspicious activity are recorded in the ticketing system. Validate that system components audit all of the required auditable events.

Technology specific: General

**AU-3: Content of Audit Records**

NIST SP 800-53 Objective: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Control Translation: This control is to ensure that the component audit records contain the required information for each recorded event.

How to test and evaluate: Obtain 5 raw audit logs from the component (syslog, error log, authlog, event log). If a centralized audit tool is utilized, the evidence should also be collected form the tool and compared to the raw log. Examine the audit logs to ensure the records detail the following:

Type (new user creation, password reset, policy update, configuration change)

When (Data and Time)

Where (the IP address)

Source (the action that caused the event in the log)

Outcome (Success or Failure)

Associated identity (user identifier, device identifier, process)

Technology specific: All components

**AU-4: Audit Storage Capacity**

NIST SP 800-53 Objective: The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

Control Translation: This control is to ensure that sufficient storage capacity exists on the components to allow for continual auditing.

How to test and evaluate: Examine organizational and component policies to determine the size required for audit storage. Obtain a screenshot showing the setting for 5 components (5 per unique component) showing the capacity for audit storage. This is usually the size of the component, as the logs are not given specific storage capacity. If they organization is using a large database or storage are network (SAN) to storage all component logs, verify that the 5 selected components (5 per unique component) are sending their logs to the database or SAN. Then verify the size of the database or SAN. Compare all sizes for storage capacity (individual component, SAN, database) to the organizational policy requirement.

Technology specific: All components

**AU-5: Response To Audit Processing Failures**

NIST SP 800-53 Objective: The information system:

a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and

b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

Control Translation: This control is to ensure that if an audit failure occurs, the proper actions are taken to immediately.

Notes: The concern for this control is to make sure if auditing stops alerts are sent to immediate action.

How to test and evaluate: Examine organizational and component policies to determine the personnel to be alerted in the event auditing stops on the components. Attempt to obtain an alert (email or ticket) sent to the correct person when auditing failed. Examine system configuration to ensure that alerts are sent to the appropriate parties when audit processing fails. Examine organizational and component policies to determine the action to be taken when audit failure occurs. Examine the obtained ticket to determine the action that occurred when the audit process stopped. Examine the audit logs to ensure the audit logs back up what is stated in the ticket.

Technology specific: All components

**AU-6: Audit Review, Analysis, And Reporting**

NIST SP 800-53 Objective: The organization:

a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and

b. Reports findings to [Assignment: organization-defined personnel or roles].

Control Translation: This control is to ensure that component level audit logs are reviewed continuously.

How to test and evaluate: Examine organizational and component policies to determine the frequency of component level audit log review and the activities that are to be specifically reviewed in the audit logs. Interview the audit log review personnel to determine how the audit log review process occurs. Obtain evidence or results (email, ticket) that the logs are reviewed in accordance with the time frame. Examine organizational and component policies to determine the personnel that audit issues and findings are to be reported. Review the 5 audit logs received in AU-3. Check the logs for the identified thresholds to ensure all issues where found. Obtain evidence that all issues where reported to the correct individual (email, tickets). Review the tickets to determine that all issues where examined and a resolution to the issue occurred.

Technology specific: All components

**AU-7: Audit Reduction And Report Generation**

NIST SP 800-53 Objective: The information system provides an audit reduction and report generation capability that:

a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

b. Does not alter the original content or time ordering of audit records.

Control Translation: This control is to ensure that audit logs are able to reviewed in an accurate manner though audit reports.

Notes: The organization may use a tool such as Splunk that is an audit parsing tool designed for report reduction and generation. If so ensure the component logs are sent to the tool and the tool is used for log review. The organization may also use script to parse through raw audit logs.

How to test and evaluate: Obtain evidence that the logs from the 5 identified testing components have been reduced and reports generated to allow for easy of review. Review the process or procedure for “reduction” or centralization of audit logs. The reports should pull directly from the logs and not alter the information. Check the raw logs against the report to ensure the information has not been altered or capture a screenshot show a setting that logs are write once and read many.

Technology specific: All components

**AU-8: Time Stamps**

NIST SP 800-53 Objective: The information system:

a. Uses internal system clocks to generate time stamps for audit records; and

b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].

Control Translation: This control is to ensure that the component is tied into a central time server to ensure consistency of audit logged information.

How to test and evaluate: Obtain a screenshot from the 5 selected components to ensure the NTP setting is pointing towards the organization internal time server. Review the audit logs from AU-3 to ensure all logged information has a date and time associated with the event. Ensure the NTP connection is resolved in accordance with the organization defined time frame listed in the organizational and component level policies.

Technology specific: All components

**AU-9: Protection Of Audit Information**

NIST SP 800-53 Objective: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Control Translation: This control is to ensure that audit logs are not alterable to cover the malicious action a user may perform.

How to test and evaluate: Obtain a screenshot from the 5 selected components to show the setting that logs are write once ready many. This means that logs can only be written to once and can’t be altered or adjusted. Many root accounts are able to alter logs. If this is true, test the root account to ensure that the only means of accessing the root account is through sudo actions. Test the obtained raw logs to ensure that all sudo activity is captured and the associated accounts are captured as well. If there is a user group that has the ability to modify audit logs, then the system should transmit the logs in near real time to a protected location as a compensating control. For example, if network administrators can modify firewall logs, then those firewall logs should be collected by a syslog server that the network administrators do not have access to.

Technology specific: All components

**AU-10: Non-Repudiation**

NIST SP 800-53 Objective: The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [Assignment: organization-defined actions to be covered by non-repudiation].

Control Translation: This control is to ensure that all activity is associated to a unique user, process, device, or system.

How to test and evaluate: Examine the organizational and component level policies to determine the actions that require non-repudiation. Examined the obtained audit logs from AU-3 and ensure that all events have an associated unique identifier associated with the event. Ensure the identifier is on the access control list (ACL) and that the identifier is only assigned to one user, process, system, or device.

Technology specific: All components

**AU-11: Audit Record And Retention**

NIST SP 800-53 Objective: The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Control Translation: This control is to ensure that component level audit records are stored for a long period of time to support after the fact investigation as needed.

How to test and evaluate: Examine the organizational and component level policies to determine the time frame for retaining audit records. Obtain a screenshot of the 5 identified components (5 per unique component) to show the setting for storing audit logs. Most components will recycle the set log space as the logs fill. If this is the case, search and locate the oldest log and capture the audit log to compare against the organizational requirement. Some organization will use a database or storage area network (SAN) to store component level logs. If this is the case, ensure the component connection to the database or SAN is active and operating as intended. Obtain a screenshot showing the connection configuration. Search the database or SAN for the component level audit logs to ensure the logs are stored for the required time frame. Take into account that some components may not have existed for the required time frame. If that is the case, capture a screenshot of the log from the component inception.

Technology specific: All components

**AU-12: Audit Generation**

NIST SP 800-53 Objective: The information system:

a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components];

b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and

c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Control Translation: This control is to ensure the component level audit logs contain all of the required auditable events listed in AU-2 and contain the specific information stated in AU-3.

How to test and evaluate: Reference the analysis for AU-2 and AU-3 for the evaluation of this control. Utilize the audit logs obtained in AU-3. During the meeting with the system administrator obtain a screenshot to show the configuration capabilities of the component. Some components do not have this capability and log all events. Review the logs from AU-3 to ensure that all events listed in AU-2 are shown in the logs and each event in the log contains the information from AU-3. Some events listed in AU-2 may not have occurred or are not possible on the component. If this is case two options are available. Option 1, obtain written permission to create the events that have not occurred at the component level. Review the logs to ensure the events manually created are contained in the audit logs. Option 2, obtain a written statement from an authority at the component level stating that the component is not able to record these events or these events are not possible at the component. The written statement should clarify why the events are not possible at the component level.

Technology specific: All components